Strategy Research Project

Future of Department of Defense Cloud Computing Amid Cultural Confusion

by

Colonel Scott A. Smith
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Future of Department of Defense Cloud Computing Amid Cultural Confusion

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Scott A. Smith
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Jeffrey L. Groh
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,218

14. ABSTRACT

The Department of Defense (DoD) is executing plans for a Joint Information Environment (JIE), and all Services have embraced this concept. Data center consolidation and information sharing are goals of the JIE. In 2012, the National Defense Authorization Act directed DoD to provide a single enterprise cloud-computing environment and transition to a public cloud service provider. Services have started the development of individual cloud-computing environments but a single cloud for all of DoD may not be the optimal solution. This research paper informs strategic leaders as the wisdom of endorsing cloud computing. It addresses related issues in matters of service culture changes and how strategic leaders will dictate the future of cloud computing. Also, in areas of data integrity, cost savings, security, and stability. It challenges the merits of the Secretary of Defense's guidance of immediately adopting a single commercial cloud technology. Furthermore, the author presents two recommendations to meet the goal of lower IT budgets through data center consolidation and individual Service provided cloud computing.

15. SUBJECT TERMS
Joint Information Environment, Data Consolidation, Data Integrity, DISA, Strategic Leaders

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	32	

USAWC STRATEGY RESEARCH PROJECT

Future of Department of Defense Cloud Computing Amid Cultural Confusion

by

Colonel Scott A. Smith
United States Army

Dr. Jeffrey L. Groh
Department of Distance Education
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Future of Department of Defense Cloud Computing Amid Cultural Confusion
Report Date:	March 2013
Page Count:	32
Word Count:	5,218
Key Terms:	Joint Information Environment, Data Consolidation, Data Integrity, DISA, Strategic Leaders
Classification:	Unclassified

The Department of Defense (DoD) is executing plans for a Joint Information Environment (JIE), and all Services have embraced this concept. Data center consolidation and information sharing are goals of the JIE. In 2012, the National Defense Authorization Act directed DoD to provide a single enterprise cloud-computing environment and transition to a public cloud service provider. Services have started the development of individual cloud-computing environments but a single cloud for all of DoD may not be the optimal solution. This research paper informs strategic leaders as the wisdom of endorsing cloud computing. It addresses related issues in matters of service culture changes and how strategic leaders will dictate the future of cloud computing. Also, in areas of data integrity, cost savings, security, and stability. It challenges the merits of the Secretary of Defense's guidance of immediately adopting a single commercial cloud technology. Furthermore, the author presents two recommendations to meet the goal of lower IT budgets through data center consolidation and individual Service provided cloud computing.

Future of Department of Defense Cloud Computing Amid Cultural Confusion

> This country is at a strategic turning point after a decade of war and, therefore, we are shaping a Joint Force for the future that will be smaller and leaner, but will be agile, flexible, ready, and technologically advanced. It will have cutting edge capabilities, exploiting our technological, joint, and networked advantage.[1]
>
> —U.S. Defense Secretary Leon Panetta

The rise in information Technology (IT) requirements within the Department of the Army (DA) and throughout the Department of Defense (DoD) has challenged strategic leaders to consider consolidation of IT services. Tighter defense budgets and future budgetary constraints require DoD leaders to seek possible commonalities for a truly joint force. The Chairman of the Joint Chiefs of Staff echoed Secretary Panetta's comments on the new strategy for the future force: "We must develop a Joint Force for 2020 that remains ready to answer the Nation's call – anytime, anywhere. We need to offset fewer resources with more innovation."[2] Then he added, "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communications networks and assured access to cyberspace and space."[3]

DoD and Defense Information Systems Agency (DISA) leaders must look for new and innovative methods to provide the force with 21st century technology. The current DoD strategy is to develop and deploy an enterprise cloud-computing environment. Although cloud computing is DoD's way of the future, it may not be the current optimal solution for DoD. This research paper informs strategic leaders as to the advisability of endorsing cloud-computing. It addresses service cultural changes and how strategic leaders will dictate the future of cloud computing. Also, in related issues of data integrity, cost savings, security, and stability. It challenges the merits of the Secretary of

Defense's guidance and the DISA's goal of immediately adopting a single commercial cloud technology.

DoD has teamed up with DISA, as the enterprise service provider, to develop the Enterprise First approach. This approach is a transformational swing from mission-particular technologies with stated procedures and tightly controlled governance rules to a unified and synchronized data-focused enterprise information environment.[4] This transformation will modernize the entire enterprise to meet the proposed DoD strategy and seek a solution that shadows private industries' practices.

DoD Information Environment

The IT landscape has evolved vastly at all levels over the last 10 years. In the 10th Mountain (MTN) Division 2003 Warfighter Exercise, 25 personnel and six servers supported the Division's IT requirements. In 2004, the Division returned from Afghanistan and immediately restructured into Brigade Combat Team (BCT) Modularity. This transformation triggered the IT challenges facing DoD today. Modularity required an increase of the BCT's IT personnel from 0 to 15. Servers increased exponentially as well. At the brigade headquarters prior to modularity, there were no servers; now there are racks of them (figure 1). The total divisional IT requirements have increased times six times throughout the division. Units demanded all of the new information they received while deployed after they returned to home station. The hunger for information grew exponentially within every echelon Army-wide and throughout DoD.

Figure 1, 1st BCT, 10th MTN DIV (LI) after modularity 2005.[5]

This sudden IT expansion has caused serious security problems throughout DoD. More importantly, it has raised problems with information-sharing through among current small islands of information. The IT footprint expanded, and the cost for new technologies continued to rise. Further, it became a cumbersome challenge to develop interfaces among these systems to share information because each service and agency had developed their own standards and processes.

Like most organizations throughout DoD, the Chief Information Officer (CIO) G6 could not stay ahead of the swiftly changing IT environment. The organization restructured to better provide DoD oversight, but it soon became evident that the newly minted organization inadvertently covers other organization responsibilities; more times

than not, it provided conflicting guidance. So providing oversight to DoD on the development and delivery of technology became an insurmountable task.[6]

DoD realized that its IT operations had devolved into a state of duplicative, cumbersome, and costly set of application silos. It needed sweeping reorganizational changes as well as a new direction that would provide more responsive, secure, and less costly IT.[7] DoD IT was not disseminating information in a timely fashion due to these separate networks. DoD must now refocus its efforts on information sharing.[8]

The total reorganization of the DoD CIO has created more malleability and less redundancy. The new smaller organization gives flexibility and enables teams to be built with up-to-date knowledge and expertise. DoD can now deliver relevant capabilities.[9] Along with this reorganization, DoD CIO teamed with DISA to develop a plan to modernize all of their IT infrastructure, processes, and personnel. The Joint Information Environment (JIE) served as the concept to modernize DoD.

As defined by the 4-Star Joint Chiefs of Staff TANK, the goal of JIE is:

> A secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).[10]

This guidance informed DoD that everything from end-to-end must be fixed. Fiscally, this was an impossible task. The office of DoD CIO offered clarifying guidance to assist and direct the actions and provide focus. This guidance identified five key areas, known as “big rocks”: The Joint Network (Network Normalization), Identity Management/Access Control, Enterprise Data Center Consolidation, Enterprise Services, Enterprise IT Governance.[11] These must-fix big rocks are four of the ten areas

that DoD CIO believes are keys to success, specified in their 10 Point Plan for IT Modernization and the successful implementation of the JIE.[12] Figure 2 provides a graphic comparison of the current DoD environment with the proposal JIE end state.

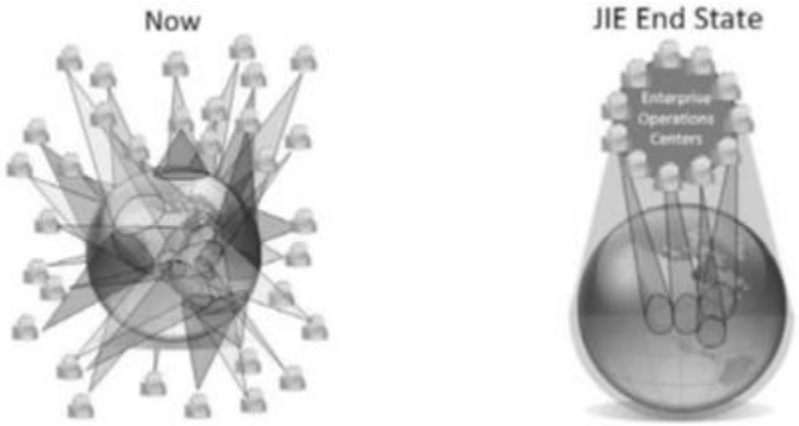

Figure 2, JIE evolution from current state to end state.[13]

One controversial element of the JIE is the Enterprise Services (ES). The goal of ES is to provide a single DoD information environment to be rapidly developed and sufficiently robust to meet the warfighter's -Army, Navy, Air Force, or Marines- needs anywhere around the world when required.[14] The most familiar current ES initiative are the DISA provided Enterprise Email and Collaboration Services. The final objective of ES is to move all DoD organizations under one DoD cloud computing-environment.

In 2012, DoD CIO released its Cloud Computing Strategy document. To build the DoD environment, it must focus on a government-owned cloud and tie it in with commercial cloud-computing providers to create an overall single IT environment.[15] Also released in that year was the 2012 National Defense Authorization Act (NDAA). This legislation directs the "migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services

generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security."[16]

Cloud Computing

The National Institute of Standards and Technology has defined cloud computing as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[17] There are a number of different types of clouds: Private Cloud would be DoD-owned and operated; Public Cloud is owned and operated by a commercial company; Hybrid Cloud shares data among multiple clouds. Whether a public, private, or a hybrid cloud, every cloud provider provides its services through one of three means. They are Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS). Regardless of the cloud, these services differ in their owner and their managers.[18]

To meet the NDAA 2012, DoD must migrate to a Public Cloud in a PaaS environment. According to the current DoD CIO Cloud Strategy reads, DoD will design a Hybrid Cloud that operates in a SaaS environment; it will maximize the use of commercial providers whenever possible. Any successful cloud environment design designates a group to manage the transition from its current computing environment to a cloud-computing environment. The responsibility for the facilitation resides with a cloud broker. According to Gartner's Daryl Plummer, the broker is usually an outside party that serves an intermediary between the cloud provider and the end user. The broker is a valuable asset; it coordinates the customer's needs with the service providers to assure that the service support the organizations functions.[19] DoD has

described its broker as an “entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumer.”[20] DoD will use a broker as a facilitator between other government agencies and commercial service providers, but not between the users and the DoD cloud provider. In July 2012, DoD announced that DISA will assume the responsibilities of the DoD Cloud Computing Provider and the Cloud Computing Broker.[21] This indicates DoD plans for only negligible flexibility in the design and participations from the customer’s point of view to transition into the DISA cloud.

The cloud-computing methodology is now the responsibility of DISA which will implement the technology, migrate current operations into cloud-computing, and manage the new system. The DISA goal is to ”Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department’s mission, anywhere, on any authorized device.”[22] DISA has adopted the DoD Cloud Computing Strategy as its guiding document for developing an environment that will allow all components and agencies to maximize their use of other component’s cloud services.[23] Accordingly, DoD will permit multiple cloud providers to operate within the JIE environment. However, this falls short of achieving a single DoD/DISA Enterprise Cloud.

DoD identified four critical areas that require action in its cloud-computing strategy. First, the strategy should foster the adoption of cloud-computing. Acceptance of cloud computing means DoD must accept all aspects of IT governance for the cloud. DoD leaders must advocate the cultural change that an enterprise cloud will bring about. The cloud computing environment needs recognition and endorsement from

strategic leaders throughout DoD. Second, the strategy must optimize data center consolidation. IT managers must comply with the 2010 Secretary of Defense Directive to consolidation of the IT footprint. Consolidation of data is a primary component of a cloud computing. Consolidation means more than moving data; it also requires manipulating and preparing the data to function within a cloud environment. Third, IT leaders must establish the DoD enterprise cloud infrastructure. Optimizing the data to ensure that it is scalable will facilitate the swift development and release of commercial off the shelf (COTS) applications and services. Fourth, IT leaders must deliver cloud services. After developing future capabilities, it is imperative to incorporate legacy data along with other government and commercial cloud environments.[24] These four steps along with fulfilling the DoD 10 Point Plan to IT Modernization will produce an effective leap into the DoD Cloud Computing Environment.

With the approved and published strategy to transition DoD departments to an enterprise cloud environment, DISA is now primed to provide a fully synchronized and resilient single enterprise. There are, however, other difficulties that DoD faces besides financing this conversion. This research addresses the skepticism of some experts who question the practicability of cloud-computing. These challenges come in the areas of security, data integrity, cost, and stability. The biggest challenge that will face DoD is the requisite cultural shift within the Services and management of this massive change. The success of cloud computing finally depends on the actions and attitudes of DoD Strategic Leaders.

Cultural Changes

Three critical competencies exist for those strategic leaders who will execute a robust top-down approach for successful cloud computing. The U.S. Army War College's Strategic Leadership Primer defines strategic leadership as:

> The process used by a leader to affect the achievement of a desirable and clearly understood vision by influencing the organizational culture, allocating resources, directing through policy and directive, and building consensus within a volatile, uncertain, complex, and ambiguous (VOCA) global environment which is marked by opportunities and threats.[25]

So strategic leaders must then focus on influencing others through processes to achieve an end state by consensus at the highest level.

Strategic leaders' vision aligns their organizations from the strategic level to the lowest tactical level and all departments in between. DISA has provided the vision of an enterprise data environment. It developed a roadmap depicting the direction the organization must travel to reach its envisioned destination.

The ability to facilitate change is the next strategic leader competency. Change is inevitable. If change does not happen, the organization remains technologically static and functionally moribund. The current DoD IT stovepipe networks of today are evidence of failure to change. In today's volatile, complex, and ambiguous environment, the organization is invariably going to fluctuate aimlessly. To provide direction, the Secretary of Defense has mandated needed change. Transformation in a large organization is enormously challenging. Leaders of change struggle against many different resistant elements. In *Leading Change*, John Kotter claims, "successful transformation is 70 to 90 percent leadership and only 10 to 30 percent management."[26] Invariably, making envisioned change requires concerted and talented leadership. When leaders dispel employers' fears and gain their confidence in the merits of the

change, the employees will support the change. The ideal way for change to happen is through a team effort. The Army proved it has the adaptability to undergo major change when it transformed from division-centric brigades to the new modular brigade combat teams.

Cultural and organizational change is needed to achieve the goal of the enterprise. DISA initiated the change process by identifying the requirement for common sets of standardized practices and procedures for all the services. To achieve this commonality, DISA urges all services and agencies to change how they operate and conduct business. This gargantuan change is tantamount to a complete service cultural change. It requires that each service must now act and look and conduct their operations the same as the other their conduct of daily business and the way they provide IT services.

In 2011, Teri Takai the DoD CIO, in an interview with Federal News Radio responded, “that the Office of Management and Budget authorized DoD CIO authority to do just that to ensure that the Services CIO conform to the new Enterprise Environment.” Later in that interview, she admitted that, “She had no plans to mandate that type of cultural change.”[27] During the first discussions of implementation of a DISA Enterprise Email System, DoD realized that an enormous mindset change will be required for widespread acceptance of the new system. At the DoD level, because of Title 10 Authority, there are limited ways of forcing changes into the services. The best chance for successful for change is to socialize change and promote ideas favorable messages to gain acceptance. During the first meetings with all of the Services CIOs, it became apparent that the simple circumstances of losing the Services’ identity on their

email addresses quickly aroused nearly insurmountable opposition.[28] Dissention came first from the U.S. Marines CIO, Brig Gen Nally: “We earned the title of United States Marines, and we are damn proud of it, you can have at whatever dot-mil you want to have, but you are not changing my culture.”[29] U.S. Marine Corps has not announced their plan, if any, to move to the DISA Enterprise Mail Services. Such actions will halt the goal of an enterprise environment if our strategic leaders cannot negotiate through these cultural issues.

Consensus building is the last competency that strategic leaders will need to effect the change to cloud computing. In defining strategic leadership, nowhere do we find the term “decision-making”. The words “affecting”, “influencing”, and “building consensus” have replaced it. Effective consensus builders will not only ensure DISA’s success. More significantly, it will ensure the DoD goal remains achievable. Ironically, every concession needed to build a consensus in support of cloud-computing makes the process of implementing the designed change even more complex. Despite these concessions, DISA must be diligent in enforcing the new standards to govern the enterprise.

DoD Strategic Leaders are vital agents in introducing change. They will be responsible for leading their subordinate organizations through the initial stage of change. If they are able to maneuver through this cultural minefield, these leaders will find their work has just begun. Cloud computing is in its infancy and evolving daily. There are a several additional risks that must be addressed in the proposed transition to DoD’s goal of cloud computing.

Data Integrity

The Department of Homeland Security (DHS) has issued a warning about cloud computing in 2011 from the U.S. Computer Emergency Readiness Team. The team's advice is directed at small businesses, but is relevant for all users of cloud providers. The advisory issued to users cautioned them to know what types of information they are storing in the cloud, because they will have little or no control over the stored information. More importantly, they will have no idea who will have access to that data, including inside and outside threats.[30]

Issues exist with data integrity and the way Commercial service providers handle the data. Their storage of aggregated data of personnel identifiable information (PII) raises questions. According to Bob Brown of Network World, commercial providers claim proprietary right to the architectural design of their storage software. Most providers claim storage issues are no longer the customers' concern once they move data into the providers' facilities. Instead they claim the data now belongs to them.[31] Service providers claim that once data becomes their responsibility, they can store it anywhere within their data centers, at any location around the world in accord with the providers' best practices. Another concern is that providers' consolidation of some unclassified data stored with other unclassified data will render this data as classified. Within public clouds, DoD would lose visibility of where data is stored; also, DoD could not audit this data. So it should not use a public cloud. SLAs can dictate where to store the data to meet all laws and regulations. More stringent the SLA become adds additional costs due to the provider changing how it normally operates. Accordingly, providers must develop cloud service solutions for specific organizations, so the providers cannot rely on their own best practices.

According to Wayne Rash, “cloud providers don’t meet current compliance rules. What is more, some providers, such as Amazon.com, have said that they don’t intend to meet those rules and that they won’t allow compliance auditors on-site.”[32] When the largest and most respected cloud provider openly defies regulatory regime, smaller providers may follow suit. An SLA offers no assurance that DoD data will reside within the United States and not in a foreign location. Companies operate to stay in business and make money for their stockholders. If their current policies lose them business, they may change their policies to assure greater security for their users.

Cost Benefits

At an Armed Forces Communications and Electronic Association symposium, Mike Krieger, Army Deputy CIO/G6, commented on costs associated with enterprise e-mail. He reported that DoD now has visibility of the cost per user for this service because DISA must identify this cost in the president’s budget. DISA’s published estimate for 2011 was $52 per user. Recent analysis indicates that this cost has increased to $150 to $190 per user.[33] The discrepancies in numbers are not the issue. But DoD must ensure that the estimates for the general enterprise concept are as accurate as possible.

DoD CIO is striving to identify savings through the programs of JIE and server consolidations. The individual Services have already begun realizing these savings. The Army has over 300 data centers; it is executing a plan to move and consolidate to 225 centers, which will yield $1.5 billion in annual savings.[34] The Navy announced in December 2012, that, in conjunction with the Marines, they have already reached $100 million in savings from their consolidation of 160 to 25 data centers; over the next five years, they anticipate additional savings.[35] The Air Force has been consolidating its data

centers since the early 2000. So the services are well underway in designing and executing internal plans for consolidation. The next step must be assessments of possible gains, despite the additional stand-up costs, associated with the further development and consolidation of data centers again at the DISA level.

Currently, each Service is moving to a private service cloud. The Army received approval to spend $249M to deploy a private cloud.[36] The Navy is in its final approval process to begin execution of its $1.9B Next Generation Enterprise Network.[37] In 2010, the Air Force has joined forces with IBM to develop a cloud pilot.[38] With the Services already actively planning and using cloud services, DoD must justify the advantages of expending further upfront costs to develop and deploy an additional DISA-sponsored single enterprise cloud environment. No matter which cloud-computing environment chosen, the predominant challenge is the security of the system.

Security

According to President Obama's 2010 U.S. National Security Strategy (NSS), cyber security threats pose the most serious national security, public safety, and economic challenges facing the nation. Defense against cyber-attacks requires networks that are secure, trustworthy, and resilient. The U.S. Government (USG) must protect the digital infrastructure as a strategic national asset. But the USG alone cannot assure cyber security. Only a holistic government-led approach will secure the nation's assets.[39] In fact, U.S. national security is essentially dependent on the world's weakest computer system. Because of the sophistication of both state and non-state actors and this nation's antiquated technologies, standards, and regulations, it is difficult to identify where current attacks originate and to recognize the attackers. More than governments

are vulnerable. Consider the 2009 Night Dragon cyber-attack. This primitive but effective attack targeted global oil, energy, and petrochemical companies.[40]

The United States has been the target of increasingly sophisticated attacks over the years. According to the Director of National Security Agency, attacks on the U.S. infrastructure have risen 17-fold since 2009.[41] These attacks target the entire critical U.S. infrastructure, not just DoD. For example, a 2012 attack targeted the South Carolina Department of Revenue; it affected 3.6 million residents as well as the Department itself.[42] Likewise, a focused attack in 2006 shut down the U.S. Naval War College.[43] Another 2006 attack on the State Department compromised U.S. embassies worldwide, as well as in Washington.[44] Finally, the 2009 Ghostnet cyber espionage ring penetrated 1,200 systems in 103 different countries.[45]

The cyber security threats against DoD and the nation have not gone unnoticed by DoD leadership. Henry Sienkiewicz, Vice Chief Executive for Information Assurance, acknowledges the gravity of cyber threats. He believes cloud computing will create more security hurdles. He predicts that DISA's role will grow.[46] Regina Dugan, Director of the Defense Advanced Research Projects Agency (DARPA), wastes no words: "The potential capability for cyber mayhem makes cyber security one of the most intense challenges of our time." DARPA has increased it information assurance budget by $88M for testing IA technologies to address these challenges.[47]

The creation of U.S. Cyber Command (CYBERCOM) clearly indicates DoD's consciousness of the threat. CYBERCOM will retain the responsibility to protect the DoD network, including a DOD Private Cloud. The security challenge becomes more formidable within a public cloud. CYBERCOM will lose security control of DoD data

stored in a commercial service provider. The DoD strategy focuses on cloud computing at the end user level as it continues to develop two-factor authentication, data encryption, and re-training of IT System Technicians into Information Assurance Specialists. CYBERCOM will continue to do the heavy lifting for cyber defense.[48]

The NSS states that cyber security is vital, yet the NDAA directs the consolidation of services and the transition to public service providers. NDAA assumes that commercial providers offer better security than DoD is capable of providing. In January 2013, the USG disclosed that nine major U.S. banks had been under cyber-attacks in a sophisticated denial-of-service attack for a number of weeks. The difference from the past attacks was that the attackers commandeered a whole cloud and then used the cloud's own computing power against itself.[49] Every day DoD repels cyber-attacks against its networks, but no DoD data centers or clouds have been seized as the manor the of banking system clouds. It is questionable to assume that public providers are more secure than DoD networks. Operating in a single cloud environment, DoD would be incredibly vulnerable to this kind of attack launched a few months ago on U.S. banks.

Stability

As DoD moves to cloud computing, the final concern is the stability of the service providers' data centers. This stability resides in quick access to data and unquestioned assurance of its omnipresent availability. These concerns apply to both public and private clouds. Natural or manmade disasters or simply hardware or software problems can expose vulnerabilities. Many outages have occurred in the last few years, but as technology and service providers' processes improve, these outages should decrease. Among the biggest outages in 2012 were these of GoDaddy, Salesforce.com, Dropbox,

Google Talk, Googles, Microsoft Office 360 (twice), Microsoft Windows Azure, and Amazon (twice).[50] The latest outage happened on Christmas Eve 2012, during which Amazon experienced a 24-hour outage.[51] Each of these outages lasted only hours, yet they had major effects. Commercially, these outages can mean losses millions of dollars. But for DoD, they could cause a catastrophic loss of national security. DoD may not be able to provide flawless reliable and secure cloud services. But commercial sector has exhibited serious weakness in both the reliability and security of its cloud computing.

Recommendations

Recommendation 1

The author recommends the Services preserve their Title 10 Authority and retain the responsibility for the Server Consolidation. Further, Services must continue to develop and manage their own private individual cloud computing environments.

The advantages of executing this recommendation is DoD will capitalize in several areas. First, cost savings have been realized through the services' consolidation IT assets, and through further consolidation of an additional 360 data centers.[52] The DISA Strategic Plan, Key objective 1.1, identifies the merging of the enterprise through the consolidation of data centers.[53] DISA has not released a cost estimate on the overall funding required facilitate it data center goal. However, to consolidate each of the services, a large facility will be required. By each department maintaining its own data centers, DoD will strategically benefit through cost avoidance by requiring no additional funds for a larger facility. The second advantage is that DoD will again recognize savings through cost avoidance for services to provide individual private clouds. Recently the Army announced its plan for spending $249 million for the development a

cloud computing environment.[54] DISA has not announced to the public their cost estimate for a single DoD enterprise cloud. However, for providing only two of the enterprise services there is a cost estimate of $100 million a year.[55] This leads to an educated assumption the cost of integrating all of DoD's data to a DISA cloud will be exponentially higher. Commercial service providers will add further costs for manipulating data to fit within their individual public cloud best practices. The third advantage of individual cloud environments is it eliminates the potential for service culture battles that could jeopardize the entire cloud-computing and data consolidation effort. Finally, by utilizing a more secure cloud environment, the strength of DoD information defense, CYBERCOM, is assured.

A disadvantage of this proposal is the DoD will fall short in meeting the NDAA directive to deploy a commercial cloud or a single enterprise cloud. However, it will meet the intent of server and data consolidation. It also gains the advantage of commercial best practices.

The recommendation to provide individual private clouds, offers the least amount of operational risk to DoD due to the overall strategic cost. By keeping three individual service clouds verses one enterprise public cloud DoD will achieve savings through cost avoidance. Also, it provides the least amount of institutional risk to the entire enterprise as an outage to one particular area of the system and not the entire DoD network.

Recommendation 2

DISA must remain focused on IT Governance. The key to success of the enterprise is the effort placed on the development of standards and oversight. Whether the decision to move forward with a single public cloud or a single enterprise environment with multiple service clouds.

The advantage of IT governance and the need for data standards will become evident during the development of new applications. DoD will recognize lower development costs as software designers begin design with a known environment. Strong identified standards allows for information sharing to occur between the clouds and required to move to a single cloud.

A disadvantage is DoD will lose an organization to enforce the new standards and ensure proper implementation. Mitigation of the risk is DISA providing quality oversight throughout the process.

Through resilient IT governance process ensures no degradation in the DoD environment or future challenges risks due to Services applying individual standards. Also, strict governance will shape the enterprise environment for future incremental pursuit of the end state of a single public cloud computing environment. The operational risks to DoD are minimized. Standards will optimize the effectiveness of information sharing and allow commanders the capabilities to perform their interagency and multination missions. The institutional risk if DoD does not adhere to the recommendation, will lead to an environment filled with software patches developed to repair interoperability shortfalls. Over time, large numbers of software fixes will lead to a slow and inefficient cloud.

Conclusion

The DoD in partnership with DISA announced their strategic goal of transforming the enterprise IT environment to facilitate collaboration among the Services and other government agencies. The release of the NDAA in 2012 mandates the DoD to consolidate its IT infrastructure and transition it to more stable and secure public service providers. The Services are executing consolidation of data centers and eliminating

cumbersome stovepipe IT systems. Services have begun development and procurement of individual service cloud-computing environments. The missing link for complete collaboration between the Services is IT governance.

In a time of austere budgets departments must review and adjust their strategic direction and thinking on how to reduce IT spending and keep data secure and available. The DoD can reduce its expenditure through cost avoidance by accepting the recommendation of Services continuing to consolidate and deploy individual private cloud environments. Also, DISA's focus and efforts must be on IT governance. Common data standards provide will improve the combatant commands ability to maximize collaboration and data sharing.

By accepting these adjustments to the strategic goal and end state, DoD is staged to design a single enterprise environment with multiple private clouds. This newly designed DoD environment is prepared to transition to a public cloud once they mature and develop better security and stability. There are two areas that require further research for DoD to achieve the stated strategy on cloud-computing. First, how will DoD provide security to data stored in a commercial data center. A number of effective security measures exist, but each carries associated risks. A mitigation strategy needs careful consideration and planning. Second is users accessing data anywhere, on any device (e.g., mobile devices) carries its own unique security challenges. Both identified research topics exceeded the scope of this paper.

Endnotes

[1] U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense*, (Washington, DC: U.S. Department of Defense, January 5, 2012).

[2] U.S. Defense Information Systems Agency, *Strategic Plan 2013 – 2018 version 1*, (Ft Meade, MD, 2012), 2, http://www.disa.mil/About/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 28 December, 2012).

[3] Ibid.

[4] U.S. Department of Defense, *Chief Information Officer, Cloud Computing Strategy* (Washington, DC: U.S. Department of Defense, July 2012), 12, http://www.disa.mil/Services/~/media/Files/DISA/Services/Cloud-Broker/dod-cloud-strategy.pdf?new (accessed 22 October 2012).

[5] Photograph taken by the author of this paper while stationed at Fort Drum NY, serving as the Division Automation Management Officer (DAMO) for the 10th Mountain Division (Light) Infantry Division in April 2005. The Photograph taken is of the final fielding of the 1st Brigade Combat Team Tactical Operation Center. The responsibility of the DAMO is developing and fielding of all automation requirements throughout the division in close coordination with DA G6 during the Army transformation process.

[6] U.S. Department of Defense*, DoD CIO Campaign Plan, Version 1* (Washington, DC: U.S. Department of Defense, November 2012), 6.

[7] U.S. Department of Defense, *Chief Information Officer, Cloud Computing Strategy*, E1.

[8] Claudette Roulo, "Official Describes Joint Information Environment," *U.S. Department of Defense Information* (October 3, 2012): 1, in ProQuest (accessed October 2012).

[9] U.S. Department of Defense, *DoD CIO Campaign Plan, Version 1*, 7.

[10] U.S. Department of Defense, *Joint Information Environment Operations Concept of Operations* (Washington, DC: U.S. Department of Defense, October 18, 2012), 6.

[11] U.S. Department of Defense, *DoD CIO Campaign Plan, Version 1*, 11.

[12] Ibid., 9-10.

[13] U.S. Department of Defense, *Joint Information Environment Operations Concept of Operations*, 10.

[14] Ibid., 33.

[15] U.S. Department of Defense, *Chief Information Officer, Cloud Computing Strategy*, 1.

[16] 112th Congress of the United States, *National Defense Authorization Act, 2012* (Washington, DC: U.S. Government Printing Office, 2012), 409.

[17] Peter Mell and Timothy Grance, The National Institute of Standards and Technology, Definition of Cloud Computing, Special Publication 800-145 (Gaithersburg, MD: U.S. Department of Commerce, September 2011), 2, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed January 2013).

[18] Ibid., 2-3.

[19] Daryl Plumber, Gartner INC, "The Business Landscape of Cloud Computing," 2012, http://www.ft.com/cms/5e231aca-a42b-11e1-a701-00144feabdc0.pdf (accessed January 2, 2013).

[20] U.S. Department of Defense, *Chief Information Officer, Cloud Computing Strategy*, C-4.

[21] U.S. Department of Defense, *DOD Releases Cloud Computing Strategy; Designates DISA as the Enterprise Cloud Services Broker* (Washington, DC: U.S. Printing Office, July 2012), http://www.defense.gov/releases/release.aspx?releaseid=15435 (accessed 13 Nov 2012).

[22] Ibid., 2.

[23] Ibid., 23.

[24] Ibid., 10 – 23.

[25] Stephen J. Gerras, ed., Strategic Leadership Primer (Carlisle, PA: U.S. Army War College, 2010), 2.

[26] John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 26.

[27] Jared Serbu, "Takai: DoD CIO can't 'mandate' culture change," *Federal News Radio*, August 22, 2011, http://www.federalnewsradio.com/239/2507740/Takai-DoD-CIO-cant-mandate-culture-change (accessed December 4, 2012).

[28] Ibid.

[29] Ibid.

[30] U.S. Computer Emergency Readiness Team, *The Basics of Cloud Computing,* (Washington, DC: U.S. Department of Homeland Security, 2011), 3-6, http://www.us-cert.gov/reading_room/USCERT-CloudComputingHuthCebula.pdf (accessed 4 January 2013).

[31] Bob Brown, "5 Cool Cloud Computing Research Projects", *Network World Newsletter*, (June 10, 2009), http://www.networkworld.com/news/2009/061009-cloud-computing-research-projects.html?page=1 (accessed November 20, 2012).

[32] Wayne Rash, "Is Cloud Computing Secure? Prove it," *eWeek 26*, issue 16 (September 2009): 8, 10, in ProQuest (accessed 12 November 2012).

[33] Amber Corrin, "Army Enterprise E-mail bring new Transparency," *FCW The Business of Federal Technology*, February 22, 2012, http://fcw.com/articles/2012/02/22/emerging-technologies-krieger-army-enterprise-email-update.aspx (accessed 20 December 2012).

[34] John Foley, "How to Return $1.5B In Army IT Funding," *InformationWeek,* 1318 (November 28, 2011): 26, in ProQuest (accessed December 5, 2012).

[35] Nicole Blake Johnson, "Navy, Marines Hit IT Savings Goal Early," *DefenseNews*, December 3, 2012, http://www.defensenews.com/article/20121203/C4ISR01/312300001/Navy-Marines-Hit-Savings-Goal-Early (accessed January 4, 2013).

[36] Chathan: Newstex, U.S. Army Grants HP $249 million contract to deploy cloud Services, *Engadget – BLOG* (April 3, 2012), in ProQuest (accessed 23 October 2012).

[37] Henry Kenyon, "Navy Readies NGEN for Prime Time," *Defense Systems,* November 12, 2010, http://defensesystems.com/articles/2010/11/17/defense-it-2-ngen-acquisition-ready-for-prime-time.aspx (accessed January 6, 2013).

[38] Rutrell Yasin, "Air Force, IBM plan to Demonstrate Secure Cloud Computing," *DefenseSystems,* February 5, 2010, http://defensesystems.com/articles/2010/02/04/air-force-ibm-cloud-computing.aspx (accessed January 6, 2013).

[39] Barack H. Obama II, *2010 National Security Strategy* (Washington, DC: The White House, May 2010), 7, 14-16, 27.

[40] Peter Piazza, "Global Energy Cyberattacks: "Night Dragon," *CSO Roundtable*, February 10, 2011, https://www.csoroundtable.org/knowledge/global-energy-cyberattacks-night-dragon (accessed October 29, 2012).

[41] Sanger and Schmitt, "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure," *New York Time*, July 26, 2012, http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=0 (accessed November 11, 2012).

[42] Robbie Brown, "Hacking of Tax Records has put States on Guard," *New York Times*, November 5, 2012, http://www.nytimes.com/2012/11/06/us/south-carolina-tax-hacking-puts-other-states-on-alert.html?_r=0 (accessed November 11, 2012).

[43] "Chinese hackers prompt Navy College site closure" *Washington Times*, November 30, 2006, http://www.washingtontimes.com/news/2006/nov/30/20061130-103049-5042r/?page=all#pagebreak (accessed on November 11, 2012).

[44] Robin Wright, "State Dept. Probes Computer Attacks," *Washington Post*, July 12, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/07/11/AR2006071101032.html (accessed November 11, 2012).

[45] John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, March 28, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all (accessed November 11, 2012).

[46] Kimberly Johnson, "DISA looks to the Cloud for Answers to DoD's Enterprise," *Defense Systems*, November 15, 2012 (accessed December 21, 2012).

[47] Gerry J. Gilmore, "DoD, Industry Address 'Intense Challenges' of Cyber Security," U.S. Department of Defense Information Agency (November 7, 2011) in ProQuest (accessed November 12, 2012).

[48] U.S. Department of Defense*, DoD CIO Campaign Plan, Version 1*, 7, 24 – 25.

[49] Nicole Perlroth and Quentin Hardy, "Bank Hacking was the Work of Iranians, Officials Say," *New York Times,* January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?adxnnl=1&ref=technology&adxnnlx=1357863958-Mky5JVVaBDGgOvcoFln3RA (accessed January 8, 2013).

[50] Jack McCarthy, "The 10 Biggest Cloud Outages of 2012," *CRN*, (December 18, 2012), http://www.crn.com/240144284/printablearticale.htm (accessed December 21, 2012).

[51] Sam Forgione, "Netflix suffers Christmas Eve outage, points to Amazon," NBC News, December 25, 2012, http://www.nbcnews.com/technology/technolog/netflix-suffers-christmas-eve-outage-points-amazon-1C7662774 (accessed December 26, 2012).

[52] Endnotes 33 and 34 identify the U.S. Army currently executing their plan for the consolidation of 225 out of 300 data centers currently in operation. The U.S. Army expects savings of $1.5 billion through consolidation. The U.S. Navy publically announced it in conjunction with the U.S. Marine Corps have reached $100 million savings through data center consolidation. Further savings expected through the consolidation of an additional 135 centers.

[53] U.S. Defense Information Systems Agency, *Strategic Plan 2013 – 2018 version 1*, 9.

[54] Refers to Endnote 35 on the U.S. Army contract award for $249 million for the development of a cloud computing.

[55] Greg Slabodkin, "DISA Offers Details on the Enterprise and Data-Center Consolidation, *Defense Systems*, May 4, 2012, http://defensesystems.com/articles/2012/04/24/cover-story-disa-initiatives.aspx, (accessed February 19, 2012)